

REMARKS

Claims 1-28 and 50-51 are pending in the present application. In the above amendments, claims 1, 11, 14, 19, 22, 26, 50, and 51 have been amended to clarify the claimed subject matter. Claims 4 and 25 are cancelled. New claim 52 has been added.

Claim Rejections – 35 USC § 112

The Final Office Action rejected claims 1, 4, 22, and 25 under 35 U.S.C. §112, second paragraph, as being indefinite since it is unclear if the first private key is disabled when the second private key is re-created or if it is disabled when the second private key is used for authentication.

Applicant has amended independent Claims 1 and 22 and cancelled Claims 4 and 25 to clarify the claims. These amendments are sufficient to overcome this rejection.

Claim Rejections – 35 USC § 101

The Final Office Action rejected claims 14-21 under 35 U.S.C. §101 because the invention is alleged to be directed to non-statutory subject matter since the specification “defines the means to include software **only** [0064].” The Examiner continues to assert that merely because the specification mentions “software” in paragraph [0064] that this makes claims 14-21 non-statutory subject matter. However, this is the wrong legal standard.

Under 35 U.S.C. Section 112, Paragraph 6, an “[e]lement in a claim may be expressed as a means ... such claim shall be construed to cover corresponding structure, material, or acts described in the specification.” The preamble of independent claim 14 clearly recites “[a] **mobile user device**” Therefore, it is clear that claims 14-21 are directed to hardware and any interpretation under 35 U.S.C. Section 112, Paragraph 6 should be limited to hardware. To ignore the plain language of the claims (in favor of contrary language in the specification) is inconsistent with, and lacks foundation in, the law.

Additionally, in the *Bilski* decision, the Supreme Court enunciated a machine or transformation test in which a claimed process is patent-eligible under § 101 if: (1) it is tied to a **particular machine or apparatus**, or (2) it **transforms a particular article into a different**

state or thing. Claim 14 is clearly tied to a machine or apparatus (i.e., “mobile user device”). Additionally, the limitations of claim 14 also transform a particular article into a different state (e.g., “means for wirelessly outputting a plurality of shares of the second private key to a plurality of different entities ...” and “means for wirelessly outputting the second public key to a verifier device ...”). Therefore, it is clear that claims 14-21 recite patentable subject matter.

Claim Rejections – 35 USC § 103

The Office Action rejected independent claims 1-9, 11-14, 16-28, 50 and 51 under 35 U.S.C. §103(a) as being allegedly obvious in light of U.S. Patent No. 5,761,306 (hereinafter “Lewis”) in view of U.S. Patent Publication No. 2003/0081785 (hereinafter “Boneh”).

These rejections are respectfully traversed in its entirety.

The Office has the burden under 35 U.S.C. § 103 to establish a prima facie case of obviousness. In *re* Piasecki, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984). To establish a prima facie case of obviousness, four basic criteria must be met. Obviousness is a question of law based on underlying factual inquiries, which inquiries include: (A) determining the scope and content of the prior art; (B) ascertaining the differences between the claimed invention and the prior art; (C) resolving the level of ordinary skill in the pertinent art; and, if applicable, and (D) secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966).

Applicants respectfully submit that the present claims are not obvious in view of the cited references under a *Graham* analysis. More specifically, one of ordinary skill in the art would not arrive at Applicant’s claimed invention in view of the differences between the cited reference and the presented claims.

By way of illustration, but not limiting the scope of the claims, Applicants disclose a system and method for *authentication* of subscriber user devices (e.g., mobile phones) with a network verifier. Each mobile user device generates its own first public-private key pair (and a backup or second public-private key pair) and *wirelessly distributes* the public key to the verifier for future *authentication* of the mobile user device. A *plurality of shares* of the second private key are wirelessly transmitted to a *plurality of different entities* once such that the second private key can be *re-created by the mobile user device to replace use of the first private key and disable the first private key when the second private key is re-created*.

A. Scope of the Prior Art

Lewis (U.S. Patent No. 5,761, 306) discloses a method in which a key server provides an active public key and a hashed replacement public key to nodes of a network. Each time a key replacement is performed, the active public key is discarded and the replacement public key replaces the active public key. (Col. 3, lines 21-32). Importantly, corresponding private keys are generated for the public keys; however, such private keys are not distributed to the nodes.

Boneh (U.S. Patent Publication No. 2003/0081785) discloses a distributed private key generating scheme used to protect a master key. In particular, the master key may be made up of a plurality of shares (s shares in Z_q , where Z_q is a group of shares under addition modulo q). (See Paragraphs [0041] and [0253]). A private key d_{ID} is generated by giving each of a plurality of private key generators (PKGs) one share s_i of the master key. (See FIG. 5) Each private key generator (PKG) then uses its share s_i to generate a corresponding private key share d_i . The private key shares d_i may then be collected by a user and combined to calculate the private key d_{ID} . (Paragraph [0253] lines 10-19).

B. Differences Between Claimed Invention and Prior Art

As to independent claims 1, 14, and 22, the Final Office Action relies on Boneh as disclosing that “it is desirable to protect the private key and to protect the key by distributing it among a plurality of different entities, and then constructing the key by requesting the shares from the entities (page 14, paragraph 253).”

The present claims recite “creating a second private key ... at the mobile user device” and “wirelessly transmitting a plurality of shares of the second private key to a plurality of different entities once ...” Consequently, as claimed, the second private key is created first at the mobile user device and then shares of the second private key are distributed to different entities for storage. The mobile user device subsequently collects the shares of the second private key to reconstruct the second private key.

By contrast, a close reading of Boneh reveals that a plurality of different shares of a master key (not the private key) are distributed to different private key generators (PKG), e.g., on different nodes. (See FIG. 5 and Paragraph [0253] lines 10-19). Each PKG then uses its share s_i

of the master key to generate a private key share d_i . A plurality of private key shares d_i are then collected and combined to form the private key. Consequently, a private key is not generated at the mobile user device distributed as claimed. Therefore, shares of the private key are never distributed by the mobile user device as claimed. Instead, in Boneh, different shares of a master key are distributed to a plurality of private key generators (PKGs), and each private key generator utilizes its share of the master key to independently generate a share of the private key.

Applicant also notes that while Lewis discloses distributing a public key and a replacement public key, Lewis does not distribute shares of its private key to other nodes. Consequently, neither Boneh nor Lewis, alone or in combination, disclose the claimed invention.

C. Level of Ordinary Skill in the Pertinent Art

Applicant further submits that the level of ordinary skill in the art would not have resulted in the asserted combination of Lewis and Boneh to disclose the claimed invention. the approaches used by Lewis and Boneh are inconsistent with each other and there would be no motivation to combine them. In particular, while Lewis discloses the distribution of active and replacement public keys, Lewis does not distribute corresponding private keys to other nodes. Boneh is aimed at protecting a master key when used for private key generation. Boneh distributes different shares of the master key among a plurality of private key generation sites or nodes which then independently generate shares of the private key that are subsequently combined to form the private key.

Consequently, while Lewis uses a centralized key server (Lewis FIG. 1, key server 16) to generate the private keys (FIG. 1, element 30), Boneh discloses that the private key should be generated as shares by distributed private key generators and subsequently combined. Therefore, one of ordinary skill in the art would not seek the inconsistent combination of Lewis and Boneh.

Claims 4 and 25

As to dependent **claims 4 and 25**, the Final Office Action relies on Lewis (Col. 3, lines 25-26) as disclosing “disabling the first private key when the second private is used for authentication of the device.” Applicant notes that the limitations of dependent claims 4 and 25

PATENT

have been added to independent claims 1 and 22, respectively, as “disable the first private key when the second private key is re-created and used for authentication.”

A close reading of Lewis reveals that “[e]ach time a key replacement is performed, the activate public key is discarded.” (Col. 3, lines 25-26). Consequently, Lewis disables the active public key when a replacement public key is generated. Lewis does not disable a **private key** when the replacement second private key is **recreated and used for authentication** as claimed.

Claim 10

As to dependent **claim 10**, the Final Office Action relies on US Patent No. 5,675,649 (hereinafter “Brennan”) (Col. 2, lines 16-31) as disclosing “preventing retransmission of the second private key.” However, Brennan refers to a very different security system that uses a master key not a private key (from a public / private key pair) as claimed. Consequently, Brennan fails to disclose this feature. Applicant submits that public / private key pair cryptographic systems are sufficiently distinct from master key systems that it would not have been obvious to apply the teachings of Brennan to a public / private key system.

The remaining dependent claims were rejected based on a combination of references, some of which are discussed above. Applicant submits that the dependent claims are novel due to their dependence on the novel independent claims. Based on at least the foregoing reasons, Applicant respectfully requests reconsideration and withdrawal of the rejection of, and/or objection and allowance of claims 1-3, 5-24, 26-28 and 50-52.

Applicant has reviewed the references made of record and asserts that the pending claims are patentable over the references made of record.

Should any of the above rejections be maintained, Applicant respectfully requests that the noted limitations be identified in the cited references with sufficient specificity to allow Applicant to evaluate the merits of such rejections. In particular, rather than generally citing whole sections or columns, Applicant requests that the each claimed element be specifically identified in the prior art to permit evaluating the references.

CONCLUSION

In light of the amendments contained herein, Applicant submits that the application is in condition for allowance, for which early action is requested.

Please charge extension any fees or overpayments that may be due with this response to Deposit Account No. 17-0026. Applicant requests a **one month** extension of time.

Respectfully submitted,

Dated: July 31, 2009

By: W. C. Kim
Won Tae C. Kim, Reg. # 40,457
(858) 651 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502